REMARKS

Reconsideration and allowance of the subject application are respectfully requested.

The Examiner rejects claims 1-4, 6, 7-9, 14-19, 20-22, 27-32, 33-35 under 35 U.S.C. §102(e) as being anticipated by U.S. Patent 6,202,153 to Diamant et al. This rejection is respectfully traversed.

To establish that a claim is anticipated, the Examiner must point out where each and every limitation in the claim is found in a single prior art reference. *Scripps Clinic & Research Found. v. Genentec, Inc.*, 927 F.2d 1565 (Fed. Cir. 1991). Every limitation contained in the claims must be present in the reference, and if even one limitation is missing from the reference, then it does not anticipate the claim. *Kloster Speedsteel AB v. Crucible, Inc.*, 793 F.2d 1565 (Fed. Cir. 1986). Diamant fails to satisfy this rigorous standard.

Diamant relates to a method for selectively connecting computer stations to a variety of computer devices in a secure fashion. As acknowledged at column 1, lines 32-33 and 39-40, Diamant addresses the problems of "securing access to data and devices when in communication over a network" and "securing an organization's networks and computers against virus programs." Diamant tries to prevent unauthorized accesses and viruses from getting into a computer system. See, for example, column 6, lines 22-24: "the communication controller 28 provides, only the secured network 8 with access to the secures [sic] storage area 24." Diamant continues:

> the communication controller 38 monitors all of the communication transmissions received from the public network so as to detect access attempts to the secured storage area 34. When such an attempt is detected, the communication controller *denies access* to the secured area 34 and executes an alert procedure to alert the user of the node.

Column 6, lines 40-45. Similar denial of access teachings can be found at column 7, lines 11-18, column 9, lines 46-53, and column 13, lines 33-45.

In contrast, claim 1 describes logic that suppresses spreading of a malware infection, which has already occurred, by disabling the input/output devices associated with that already-infected computer. Claim 1 recites "malware infection detecting logic operable to detect a malware infection of at least one computer." Diamant does not detect that a malware infection has occurred in at least one computer. In other words, claim 1 accepts that unauthorized access has occurred, not withstanding the possible use of unauthorized access prevention techniques, such as that described Diamant. Diamant does not disclose any mechanism for stopping infection from getting out of an already-infected computer.

Lacking detection of a malware-infected computer, Diamant also fails to describe the device disabling logic that is operable "upon detection of said malware infection." Similar claim recitations are found in independent claims 14 and 27. Thus, the anticipation rejection of these independent claims, and their respective dependent claims, is improper and should be withdrawn.

Claim 7 recites:

> device disabling logic operable upon receipt by a first computer of a command generated by a second computer indicative of malware infection precautions being taken external to the first computer to disable operation of one or more data I/O devices of said first computer.

The Examiner states that these claims are "rejected for the reasons set forth in the rejection of claims 1, 3 and 6."

The Examiner has apparently overlooked the fact that claims 7, 20, and 33 include claim language that is different from what is recited in independent claims 1, 14, and 27. The Examiner provides no indication where Diamant discloses the features of claims 7, 20, and 33. Nor do Applicants find these features in Diamant. Again, Diamant assumes that a malware infection has been prevented, whereas claims 7, 20, and 33 recite that a malware infection precautions have been taken external to the first computer. Where does Diamant disclose disabling one or more I/O devices of the first computer based upon receipt by the first computer of command generated by a second computer "indicative of malware infection precautions being taken external to the first computer"?

Claims 5, 10-13, 23-26, and 36-39 stand rejected under 35 U.S.C. §103 as being unpatentable over Diamant in view of U.S. Patent 6,212,635 to Reardon. This rejection is respectfully traversed.

The Examiner admits that Diamant is deficient with respect to these claims and turns to Reardon which teaches a network security system allowing access and modification by a user-plus-token technique. A security gateway 12 is a positioned in the computer bus structure between the CPU 10 and the peripherals 18, 20, and 22. A user

possessing a physical token (see column 7, lines 14-16) is able to configure the security gateway 12 of the computer to selectively block access by the CPU 10 to the peripheral devices 18, 20, and 22. Thus, Reardon only permits security level changes based on use of a physical token controlling physical hardware.

Reardon's hardware security solution is directed to an individual computer. By contrast, claims 10, 23, and 36 recite a first computer and "a second computer remote from said first computer." As a result, Reardon fails to describe features recited in these independent claims. For example, claim 23 recites the following method steps:

- receiving a first computer a user input indicative of activating precautions against a malware infection;
- upon receipt of said user input disabling operation of one or more data I/O devices of a second computer remote from said first computer.

Although Reardon may disclose certain user inputs at a first computer, Reardon fails to disclose or suggest that "upon receipt of said user input disabling operation of one or more data I/O devices of a second computer remote from said first computer."

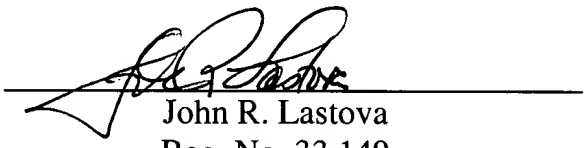
Nor would it be obvious to modify Reardon in a manner consistent with claims 10, 23, and 36. Reardon aims to prevent the computer's CPU from controlling access to the computer's peripherals because Reardon considers the action of the computer's CPU to be vulnerable to malicious control. As a result, Reardon *teaches away* from the invention described in claims 10, 23, and 36 where a remote computer selectively enables or disables I/O device access. In Reardon, such functionality would be regarded as a severe vulnerability. But the instant inventors realized that in times of high risk, a mechanism

for remotely and pre-emptively disabling I/O access in other computers provides improved overall threat protection.

For the reasons set forth above, Applicants respectfully submit that the present application is now in condition for allowance. An early notice to that effect is earnestly solicited.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: 
John R. Lastova
Reg. No. 33,149

JRL:at
1100 North Glebe Road, 8th Floor
Arlington, VA 22201-4714
Telephone: (703) 816-4000
Facsimile: (703) 816-4100